

**PERLINDUNGAN KOMUNIKASI DIPLOMATIK DI ERA DIGITAL:
RELEVANSI PASAL 27 KONVENSI WINA 1961 TERHADAP PERKEMBANGAN TEKNOLOGI**

**Muhammad Afiq Alfi Fairuz Sudirman¹, Tenri Dzulqaidah Nur²,
Nur Aprilia Umar³, Irsyad Dahri⁴**

¹⁻⁴Program Studi Hukum Bisnis, Fakultas Hukum, Universitas Negeri Makassar

¹afiqafifairuz@gmail.com, ²tenridzulqaidahnur@gmail.com, ³apriliumar03@gmail.com,

⁴irsyad.dhahri@unm.ac.id

Abstract

Digitalisation has changed the way diplomatic missions communicate with their sending States, through e-mail, messaging applications, video conferencing, and cloud-based storage. These tools make diplomacy faster, yet they also expose official communications to hacking, interception, and data breaches. This study examines the relevance of Article 27 of the 1961 Vienna Convention on Diplomatic Relations to these developments, with particular attention to Indonesia. It applies a normative juridical method, combining a statutory approach with a conceptual approach, and analyses legal materials qualitatively. The findings show that the phrase "all appropriate means" in Article 27(1) and the notion of "official correspondence" in Article 27(2) are flexible enough to cover electronic communication, provided it serves the official purposes of the mission. However, Article 27 contains no technical security standards, does not resolve questions of data jurisdiction in cloud services, and is silent on the role of private service providers. In Indonesia, the protection of digital diplomatic communication still lacks a clear legal framework and institutional coordination. The study concludes that evolutive interpretation must be accompanied by security protocols, international cyber norms, and the harmonisation of national regulations.

Keywords: diplomatic law, 1961 Vienna Convention, diplomatic communication, digital technology, cyber diplomacy

Article History

Received: October 2026

Reviewed: October 2026

Published: October 2026

Plagiarism Checker No. 234

Prefix DOI:

10.8734/CAUSA.v1i2.365

Copyright : Author

Publish by : CAUSA



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

Abstrak

Digitalisasi telah mengubah cara misi diplomatik berkomunikasi dengan negara pengirim, mulai dari surat elektronik, aplikasi pesan, konferensi video, hingga penyimpanan data berbasis cloud. Perubahan ini mempercepat kerja diplomasi, tetapi sekaligus membuka celah baru berupa peretasan, penyadapan, dan kebocoran data. Penelitian ini menelaah relevansi Pasal 27 Konvensi Wina 1961 tentang Hubungan Diplomatik terhadap perkembangan tersebut, dengan perhatian khusus pada konteks Indonesia. Metode yang digunakan ialah yuridis normatif dengan pendekatan perundang-undangan dan pendekatan konseptual; bahan hukum dikumpulkan melalui studi kepustakaan dan dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa frasa *all appropriate means* pada Pasal 27 ayat (1) dan konsep *official correspondence* pada ayat (2) cukup lentur untuk mencakup komunikasi elektronik, sepanjang komunikasi itu digunakan untuk keperluan resmi misi. Meski begitu, Pasal 27 tidak memuat standar teknis keamanan, tidak menjawab persoalan yurisdiksi data pada layanan cloud, dan tidak mengatur peran penyedia layanan swasta. Di Indonesia, perlindungan komunikasi diplomatik digital belum ditopang kerangka hukum dan koordinasi kelembagaan yang tegas. Penelitian ini menyimpulkan bahwa penafsiran evolutif perlu dipadukan dengan protokol keamanan, norma siber internasional, dan harmonisasi regulasi nasional.

Kata kunci: hukum diplomatik, Konvensi Wina 1961, komunikasi diplomatik, teknologi digital, diplomasi siber

PENDAHULUAN**A. Latar Belakang**

Negara tidak bisa berhubungan dengan negara lain tanpa perantara. Ia membutuhkan wakil yang hadir di wilayah negara tujuan, menyampaikan sikap pemerintah, mengikuti perkembangan setempat, dan melaporkan semuanya kembali ke ibu kota. Fungsi-fungsi inilah yang dijalankan misi diplomatik, dan hampir seluruhnya bertumpu pada satu hal: kemampuan untuk berkomunikasi. Misi yang tidak dapat mengirim laporan atau menerima instruksi secara aman pada dasarnya tidak dapat bekerja.

Hukum internasional sudah lama menyadari hal itu. Konvensi Wina tentang Hubungan Diplomatik 1961 menempatkan kebebasan berkomunikasi sebagai salah satu jaminan pokok bagi misi diplomatik, dan jaminan tersebut dirumuskan dalam Pasal 27. Ketentuan ini mewajibkan negara penerima untuk mengizinkan dan melindungi komunikasi bebas misi untuk semua tujuan resmi, menyatakan korespondensi resmi tidak dapat diganggu gugat, serta melarang pembukaan atau penahanan kantong diplomatik (Denza, 2016). Indonesia terikat pada ketentuan ini melalui Undang-Undang Nomor 1 Tahun 1982 tentang pengesahan Konvensi Wina mengenai hubungan diplomatik dan hubungan konsuler.

Persoalannya, rumusan itu lahir pada masa ketika kurir, telegram, dan telepon masih menjadi sarana utama. Enam dekade kemudian, wajah komunikasi diplomatik sangat berbeda. Telegram sandi digantikan surat elektronik terenkripsi, rapat bilateral berlangsung lewat konferensi video, dan arsip yang dulu disimpan dalam lemari baja kini berada di server yang letaknya mungkin ribuan kilometer dari gedung kedutaan. Perubahan ini membawa keuntungan yang nyata: pesan sampai dalam hitungan detik, rapat dapat digelar tanpa perjalanan, dan dokumen dapat diakses dari mana saja. Bjola dan Manor (2024) bahkan menegaskan bahwa digitalisasi tidak lagi sekadar alat tambahan, melainkan sudah mengubah logika dasar praktik diplomasi.

Keuntungan itu datang bersama harga yang harus dibayar. Komunikasi digital dapat diretas, disadap di tengah jalur pengiriman, disalin tanpa jejak, atau diubah isinya tanpa diketahui penerima. Peristiwa-peristiwa yang terjadi dalam satu dekade terakhir memperlihatkan bahwa ancaman ini bukan sekadar kemungkinan teoretis. Publikasi dokumen kawat diplomatik Amerika Serikat oleh WikiLeaks pada 2010 membuka ribuan komunikasi resmi ke publik. Pada 2013, pengungkapan Edward Snowden memicu pemberitaan luas tentang pemantauan terhadap misi diplomatik dan lembaga internasional. Di tahun yang sama, pemberitaan mengenai dugaan penyadapan terhadap pejabat tinggi Indonesia oleh badan intelijen Australia membuat Jakarta menarik pulang duta besarnya dari Canberra. Rangkaian kejadian itu menunjukkan bahwa isu perlindungan komunikasi diplomatik di ruang digital menyentuh hubungan antarnegara secara langsung.

Di titik ini muncul pertanyaan yang menjadi pangkal penelitian ini. Pasal 27 tidak menyebut e-mail, aplikasi pesan, ataupun komputasi awan. Apakah itu berarti komunikasi digital berada di luar jangkauan perlindungannya? Atau, sebaliknya, apakah rumusan yang sengaja dibuat longgar pada 1961 justru cukup untuk menampung teknologi yang belum terbayangkan saat itu? Kalaupun jawabannya mengarah pada yang kedua, tersisa persoalan lain: perlindungan hukum saja tidak menghentikan peretas. Ada jarak antara jaminan normatif bahwa komunikasi tidak boleh diganggu dan kemampuan teknis untuk benar-benar menjaganya.

Beberapa penelitian terdahulu sudah menyentuh persoalan ini dari sudut yang berbeda. Smărandescu (2025) menilai Konvensi Wina belum memadai untuk menghadapi ancaman siber terhadap inviolabilitas diplomatik. Al-Maadeed (2024) menyoroti Pasal 27 secara khusus dan menyimpulkan perlunya penafsiran ulang di tengah transformasi digital. Mahendra dan Triyana (2025) menelaah posisi Indonesia dan menemukan bahwa hukum nasional belum mengakui kedutaan secara eksplisit sebagai entitas yang dilindungi di ruang siber. Penelitian ini mencoba menyatukan ketiga lapis itu, yakni norma internasional, penafsirannya, dan kerangka nasional Indonesia, dalam satu analisis yang runtut.

B. Rumusan Masalah

1. Bagaimana pengaturan perlindungan komunikasi diplomatik berdasarkan Pasal 27 Konvensi Wina 1961?
2. Bagaimana relevansi Pasal 27 Konvensi Wina 1961 terhadap perkembangan teknologi digital dalam komunikasi diplomatik?
3. Apa saja tantangan hukum dalam memberikan perlindungan terhadap komunikasi diplomatik di era digital, termasuk dalam konteks Indonesia?

C. Tujuan Penelitian

1. Menganalisis pengaturan perlindungan komunikasi diplomatik berdasarkan Pasal 27 Konvensi Wina 1961.
2. Menganalisis hubungan antara Pasal 27 dan perkembangan teknologi komunikasi digital.
3. Mengidentifikasi tantangan hukum dalam melindungi komunikasi diplomatik di era digital serta merumuskan arah penguatannya.

D. Manfaat Penelitian

Secara teoretis, penelitian ini diharapkan menambah kajian hukum diplomatik, khususnya tentang cara menafsirkan perjanjian yang usianya jauh lebih tua daripada teknologi yang kini ingin diaturnya. Secara praktis, hasilnya dapat menjadi bahan pertimbangan bagi pemerintah, terutama Kementerian Luar Negeri dan lembaga yang menangani keamanan siber, dalam menyusun kebijakan perlindungan komunikasi perwakilan Indonesia di luar negeri, serta bagi mahasiswa dan akademisi yang mendalami hukum internasional.

METODE PENELITIAN

Penelitian ini tergolong penelitian hukum normatif, yaitu penelitian yang menjadikan norma hukum positif sebagai objek kajian utama (Marzuki, 2017). Metode ini dipilih karena persoalan yang dibahas pada dasarnya adalah persoalan penafsiran: bagaimana norma yang sudah ada dibaca ketika berhadapan dengan fakta teknologi yang baru.

Dua pendekatan digunakan. Pendekatan perundang-undangan (*statute approach*) dipakai untuk menelaah Pasal 27 Konvensi Wina 1961 beserta pasal-pasal yang berkaitan langsung dengannya, terutama Pasal 22, Pasal 24, dan Pasal 41, serta Undang-Undang Nomor 1 Tahun 1982 sebagai instrumen pengesahan. Telaah juga mencakup peraturan nasional yang bersinggungan dengan keamanan informasi, yaitu Undang-Undang Nomor 37 Tahun 1999 tentang Hubungan Luar Negeri, Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur

Informasi Vital, dan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi

Keamanan Siber Nasional dan Manajemen Krisis Siber. Pendekatan konseptual (*conceptual approach*) dipakai untuk memperjelas konsep-konsep seperti komunikasi resmi, inviolabilitas, kantong diplomatik, diplomasi digital, dan keamanan siber, serta untuk membangun jembatan antara prinsip hukum yang lama dan bentuk komunikasi yang baru.

Dalam menafsirkan Pasal 27, penelitian ini berpegang pada kaidah penafsiran perjanjian internasional sebagaimana tercantum dalam Pasal 31 dan Pasal 32 Konvensi Wina 1969 tentang Hukum Perjanjian, yang secara luas diakui mencerminkan hukum kebiasaan internasional. Artinya, teks dibaca menurut makna lazim istilahnya, dalam konteksnya, dan dengan memperhatikan objek dan tujuan perjanjian.

Bahan hukum primer terdiri atas instrumen internasional, putusan Mahkamah Internasional (ICJ), dokumen resmi PBB, dan peraturan perundang-undangan Indonesia. Bahan hukum sekunder terdiri atas buku, artikel jurnal, dan laporan lembaga, dengan prioritas pada terbitan lima tahun terakhir sebagai penanda perkembangan terkini, di samping karya klasik yang masih menjadi rujukan doktrinal. Bahan dikumpulkan melalui studi kepustakaan dan dianalisis secara kualitatif: ketentuan hukum diuraikan lebih dulu, lalu dihubungkan dengan karakteristik komunikasi digital dan risiko keamanannya, dan terakhir dinilai kecukupannya. Penelitian ini memiliki keterbatasan yang perlu disebut. Karena sifatnya normatif, penelitian ini tidak menguji secara empiris bagaimana kedutaan Indonesia sehari-hari mengelola komunikasi digitalnya. Praktik internal semacam itu bersifat tertutup dan sulit diakses, sehingga analisis mengenai praktik didasarkan pada peristiwa yang diberitakan secara terbuka dan pada literatur.

HASIL DAN PEMBAHASAN

A. Pengaturan Perlindungan Komunikasi Diplomatik dalam Pasal 27

Pasal 27 terdiri atas empat ayat yang masing-masing menjawab persoalan yang berbeda. Ayat (1) menyangkut kebebasan berkomunikasi. Negara penerima wajib mengizinkan dan melindungi komunikasi bebas dari misi untuk semua tujuan resmi. Dalam berkomunikasi dengan pemerintahnya serta dengan misi dan konsulat negara pengirim lainnya di mana pun berada, misi boleh menggunakan segala sarana yang layak (*all appropriate means*), termasuk kurir diplomatik dan pesan dalam kode atau sandi. Satu pembatasan ditegaskan di ujung ayat ini: pemasangan dan penggunaan pemancar radio nirkabel hanya boleh dilakukan dengan persetujuan negara penerima.

Ayat (2) menyatakan bahwa korespondensi resmi misi tidak dapat diganggu gugat, dan korespondensi resmi diartikan sebagai seluruh korespondensi yang berkaitan dengan misi dan fungsinya. Ayat (3) melarang pembukaan atau penahanan kantong diplomatik. Ayat (4) menetapkan bahwa paket yang membentuk kantong diplomatik harus memiliki tanda luar yang jelas dan hanya boleh berisi dokumen diplomatik atau barang untuk keperluan resmi.

Kalau diperhatikan, ayat-ayat tersebut menyusun dua lapis perlindungan. Lapis pertama bersifat positif: negara penerima tidak hanya dilarang mengganggu, tetapi wajib mengizinkan dan *melindungi* kebebasan komunikasi. Kata "melindungi" penting karena menunjukkan adanya kewajiban bertindak. Negara penerima tidak cukup menahan diri dari penyadapan; ia juga diharapkan mencegah pihak lain di wilayahnya, termasuk pihak swasta, mengganggu komunikasi misi. Lapis kedua bersifat negatif dan lebih konkret, yaitu larangan membuka korespondensi dan kantong diplomatik.

Pasal 27 tidak berdiri sendiri. Pasal 24 menyatakan bahwa arsip dan dokumen misi tidak dapat diganggu gugat *kanan pun dan di mana pun berada*. Frasa terakhir ini akan terbukti penting ketika pembahasan sampai pada penyimpanan data di luar gedung kedutaan. Pasal 22 melindungi lokasi fisik misi dari pemasukan oleh aparat negara penerima. Pasal 41 membebaskan kewajiban pada para diplomat sendiri untuk menghormati hukum negara penerima dan tidak mencampuri urusan dalam negerinya, dan ayat (3) pasal itu menyatakan bahwa lokasi misi tidak boleh digunakan untuk tujuan yang tidak sesuai dengan fungsi misi. Dibaca bersama, pasal-pasal ini membentuk sistem: tempat bekerja, arsip, dan jalur komunikasi misi sama-sama diberi perlindungan, sebab perlindungan salah satunya tanpa yang lain akan percuma.

Dasar pemikirannya dapat ditelusuri ke teori yang melatari kekebalan diplomatik, yaitu kepentingan fungsional (*functional necessity*). Menurut pandangan ini, perlindungan diberikan bukan demi kenyamanan pribadi diplomat, tetapi agar misi dapat menjalankan fungsinya secara efektif (Denza, 2016). Dengan kerangka itu, komunikasi dilindungi karena tanpa jaminan kerahasiaan, negara pengirim tidak akan berani mempercayakan informasi penting kepada misinya. Mahkamah

Internasional dalam perkara *United States Diplomatic and Consular Staff in Tehran* (1980) menegaskan betapa mendasarnya aturan hukum diplomatik, yang disebutnya sebagai salah satu perangkat paling tua dan paling fundamental dalam hubungan antarnegara, dan menekankan bahwa kewajiban melindungi misi bersifat mengikat tanpa terkecuali.

Penting pula dicatat apa yang *tidak* dikatakan Pasal 27. Pasal ini tidak menyebut teknologi tertentu, tidak menyebut standar keamanan, dan tidak menjelaskan bagaimana dugaan pelanggaran diselesaikan. Ia adalah norma prinsip, bukan prosedur teknis. Pemahaman ini menjadi kunci untuk bagian-bagian berikutnya, karena sebagian besar perdebatan tentang "kekurangan" Pasal 27 sebenarnya berasal dari harapan agar sebuah norma prinsip menjawab pertanyaan teknis yang memang bukan wilayahnya.

B. Relevansi Pasal 27 terhadap Komunikasi Digital

1. Penafsiran atas frasa "all appropriate means"

Argumen paling kuat bagi relevansi Pasal 27 ada pada rumusan teksnya. Para perancang memilih frasa *all appropriate means*, bukan daftar tertutup berisi sarana tertentu. Daftar yang ada, yaitu kurir diplomatik dan pesan dalam kode atau sandi, didahului kata "termasuk", yang menandakan sifatnya hanya contoh. Pembacaan ini sejalan dengan kaidah penafsiran menurut makna lazim dan objek serta tujuan perjanjian. Tujuan Pasal 27 adalah menjamin kelancaran fungsi misi; bentuk fisik sarana hanya alat. Denza (2016) dalam komentarnya menempatkan ketentuan ini sebagai jaminan yang fleksibel terhadap pergantian sarana komunikasi, dari kurir ke telegraf, telepon, dan seterusnya.

Dengan pembacaan demikian, e-mail terenkripsi, aplikasi pesan aman, dan sambungan video resmi dapat dikategorikan sebagai sarana yang layak sepanjang digunakan untuk tujuan resmi. Kata "layak" (*appropriate*) pun dapat dibaca memuat tuntutan: sarana yang dipilih sebaiknya memadai untuk memuat informasi sensitif. Artinya, penafsiran luas ini tidak hanya membuka perlindungan, tetapi juga secara implisit membebani negara pengirim untuk memilih sarana yang pantas.

Pembacaan evolutif ini juga mendapat sandaran dari Pasal 31 ayat (3) huruf (b) Konvensi Wina 1969, yang memperbolehkan praktik negara yang berlangsung belakangan dijadikan bahan penafsiran, selama praktik itu menunjukkan kesepakatan para pihak. Dalam kenyataannya, hampir seluruh negara hari ini menggunakan komunikasi elektronik dalam urusan diplomatik, dan hampir tidak ada negara yang berpendapat bahwa komunikasi seperti itu berada di luar cakupan Pasal 27.

2. Korespondensi resmi dan pendekatan fungsional

Ayat (2) mendefinisikan korespondensi resmi lewat hubungannya dengan misi dan fungsinya, bukan lewat medianya. Ini penting. Surat kertas, berkas PDF, pesan singkat, dan catatan rapat daring sama-sama dapat menjadi korespondensi resmi bila isinya berkaitan dengan fungsi misi. Ukuran perlindungannya adalah sifat dan tujuan komunikasi, bukan bentuk atau alat yang membawanya.

Pendekatan fungsional ini membawa konsekuensi praktis yang sering luput. Perlindungan tidak otomatis melekat pada setiap pesan yang dikirim seorang diplomat. Pesan pribadi diplomat kepada keluarganya, misalnya, tidak menikmati perlindungan yang sama. Dalam praktik digital, ketika satu telepon genggam dipakai untuk urusan dinas dan urusan pribadi, garis pemisahannya menjadi kabur. Persoalan ini akan dibahas lebih jauh pada bagian tantangan.

3. Analogi kantong diplomatik dan komunikasi elektronik

Ayat (3) hanya berbicara tentang kantong diplomatik, dan di sinilah analogi paling sulit ditarik. Kantong diplomatik adalah benda fisik yang dapat dikenali dari tanda luarnya. Komunikasi elektronik tidak memiliki tanda luar semacam itu, dan paket data milik misi berjalan melalui jaringan bersama pengguna lain. Komisi Hukum Internasional (ILC) dalam rancangan pasal mengenai status kurir diplomatik dan kantong diplomatik yang tidak diiringi kurir, yang diselesaikan pada 1989, sempat membahas kemungkinan bahwa kantong dapat berbentuk selain paket fisik, dan menegaskan bahwa kewajiban melindungi komunikasi resmi berlaku luas (International Law Commission, 1989). Namun rancangan itu tidak pernah menjadi perjanjian yang berlaku, sehingga nilainya terbatas pada penafsiran dan penguat doktrin.

Karena itu, jalan yang lebih aman untuk komunikasi elektronik bukan menyamakannya dengan kantong diplomatik, tetapi memasukkannya ke dalam ayat (1) dan (2). Komunikasi elektronik dilindungi sebagai *komunikasi bebas untuk tujuan resmi* dan sebagai *korespondensi resmi*, bukan sebagai "kantong digital". Pendekatan ini menghindari kebutuhan membengkokkan konsep kantong diplomatik yang secara tekstual sempit.

4. Ketentuan pemancar nirkabel dan komunikasi satelit

Satu bagian Pasal 27 ayat (1) yang jarang dibahas dalam kajian komunikasi digital adalah syarat persetujuan untuk pemancar radio nirkabel. Ketentuan itu lahir dari kekhawatiran negara penerima terhadap penggunaan siaran radio yang tidak terpantau. Dalam ekosistem hari ini, terminal satelit, perangkat komunikasi bergerak, dan jaringan nirkabel khusus yang dipasang kedutaan dapat dibaca sebagai penerus langsung dari "pemancar nirkabel" itu. Secara tekstual, instalasi perangkat semacam itu masih memerlukan persetujuan negara penerima. Ini menunjukkan bahwa kebebasan komunikasi menurut Pasal 27 tidak absolut: ada ruang bagi negara penerima untuk mengatur aspek tertentu yang menyangkut kedaulatannya, dan ruang itu tidak hilang dengan datangnya teknologi baru.

5. Pandangan para ahli: lentur namun belum cukup

Pandangan yang berkembang dalam literatur tidak seragam. Mason (2025) berpendapat Pasal 27 perlu diperbarui untuk mencakup komunikasi digital, termasuk e-mail dan sistem berbasis cloud, serta menyarankan perluasan Pasal 22 sampai 24 untuk melindungi infrastruktur digital. Al-Maadeed (2024) menyimpulkan bahwa Pasal 27 tidak memadai menghadapi transformasi digital dan membutuhkan penafsiran ulang atau revisi. Smărandescu (2025) menilai inviolabilitas diplomatik dalam konvensi belum memadai menghadapi ancaman siber, sekaligus menyarankan pengembangan norma pelengkap secara bertahap. Di sisi lain, Anjani, Susetyorini, dan Roisah (2026) berpendapat bahwa praktik diplomasi digital dapat dibenarkan melalui penafsiran teleologis tanpa amandemen formal.

Apabila pandangan-pandangan itu dibaca bersama, perbedaannya lebih bersifat tingkatan daripada pertentangan. Hampir semua sepakat bahwa *prinsip* Pasal 27 masih berlaku. Yang berbeda adalah jawaban atas pertanyaan: seberapa jauh penafsiran saja sanggup menjawab kebutuhan perlindungan, dan kapan dibutuhkan norma baru. Tabel 1 merangkum perbandingan tersebut.

Tabel 1. Perbandingan pandangan dalam literatur mengenai Pasal 27 di era digital

Penulis (tahun)	Fokus kajian	Posisi utama terhadap Pasal 27	Jalan keluar yang diusulkan	Catatan kritis
Al-Maadeed (2024)	Pasal 27 dan transformasi digital	Tidak memadai menghadapi komunikasi digital, yurisdiksi data, dan peran perusahaan teknologi swasta	Penafsiran ulang atau revisi	Menuntut perubahan relatif besar; belum banyak menjelaskan peluang penafsiran yang sudah tersedia
Smărandescu (2025)	Inviolabilitas diplomatik dan teknologi baru	Prinsip tetap relevan, tetapi perlindungan terhadap ancaman siber belum terjamin	Norma pelengkap, dikembangkan bertahap dan multipihak	Realistis secara politik, namun prosesnya panjang
Mason (2025)	Pembaruan Konvensi Wina menghadapi ancaman berbasis AI	Perlu diperbarui untuk memasukkan komunikasi digital dan sistem cloud	Perluasan Pasal 27 serta Pasal 22-24	Berupa opini kebijakan di media, sehingga bobot akademisnya lebih rendah

Penulis (tahun)	Fokus kajian	Posisi utama terhadap Pasal 27	Jalan keluar yang diusulkan	Catatan kritis
Anjani, Susetyorini, dan Roisah (2026)	Praktik diplomasi digital dan hukum Diplomatik	Diplomasi digital belum diatur eksplisit, tetapi dapat dibenarkan secara teleologis	Penafsiran teleologis tanpa amandemen formal	Cocok sebagai solusi jangka pendek, tidak menyentuh aspek teknis keamanan
Mahendra dan Triyana (2025)	Operasi siber terhadap diplomat menurut hukum Indonesia	Hukum nasional belum mengakui kedutaan secara eksplisit sebagai entitas yang dilindungi di ruang siber	Pembenahan kerangka hukum dan koordinasi kelembagaan	Fokus nasional; perlu dilengkapi analisis norma internasional

Penulis condong pada posisi tengah. Penafsiran evolutif memadai untuk menjawab pertanyaan *apakah* komunikasi digital dilindungi, tetapi tidak cukup untuk menjawab pertanyaan *bagaimana* perlindungan itu diwujudkan. Pertanyaan kedua menuntut instrumen lain, dan itulah yang dibahas pada bagian-bagian berikut.

C. Komunikasi Konvensional dan Komunikasi Digital: Perbandingan dari Sudut Pasal 27

Untuk melihat di mana Pasal 27 bekerja baik dan di mana ia tertinggal, ada gunanya membandingkan dua jenis komunikasi secara berdampingan. Tabel 2 memperlihatkan perbedaannya.

Tabel 2. Komunikasi diplomatik konvensional dan digital ditinjau dari Pasal 27

Aspek	Komunikasi konvensional (kurir, kantong, telegram sandi)	Komunikasi digital (e-mail, aplikasi pesan, video, cloud)
Wujud	Benda fisik yang dapat diidentifikasi (dokumen, kantong dengan tanda luar)	Data yang tidak berwujud, tersimpan dan berpindah melalui perangkat dan jaringan
Bentuk gangguan	Pembukaan atau penahanan fisik	Peretasan, penyadapan di jaringan, penyalinan tanpa jejak, manipulasi isi, gangguan layanan
Pembuktian pelanggaran	Relatif mudah: segel rusak atau kantong ditahan	Sulit: serangan dapat dilakukan tanpa jejak dan sering sulit diatribusikan ke negara tertentu
Pelaku gangguan	Umumnya aparat negara penerima	Dapat negara, aktor non-negara, atau pihak yang bertindak atas nama negara

Lokasi informasi	Berada dalam penguasaan misi atau kurir	Dapat berada di server pihak ketiga, bahkan di luar wilayah negara pengirim dan negara penerima
Dasar hukum paling langsung	Pasal 27 ayat (2), (3), dan (4)	Pasal 27 ayat (1) dan (2), dibaca bersama Pasal 24
Pihak ketiga	Hampir tidak ada	Penyedia layanan, operator jaringan, dan perusahaan cloud
Tolok ukur pelanggaran	Jelas secara tekstual	Memerlukan penafsiran dan standar tambahan

Tabel ini menunjukkan sesuatu yang menarik. Di baris-baris awal, perbedaannya terletak pada *cara* gangguan dilakukan, dan di sini Pasal 27 masih bisa menjangkau, sebab larangan mengganggu komunikasi resmi tidak peduli pada alatnya. Namun, di baris-baris berikutnya muncul perbedaan yang lebih mendasar: soal pembuktian, pelaku, dan keterlibatan pihak ketiga. Pada baris-baris itulah norma prinsip menemui batasnya.

D. Empat Dimensi Keamanan Informasi dan Kaitannya dengan Hukum Diplomatik

Literatur keamanan informasi lazim menilai perlindungan data melalui empat dimensi: kerahasiaan, integritas, ketersediaan, dan keaslian. Keempatnya berguna sebagai lensa untuk menilai seberapa jauh Pasal 27 dapat menopang perlindungan komunikasi digital.

Kerahasiaan adalah dimensi yang paling dekat dengan semangat Pasal 27. Larangan membuka korespondensi dan kantong diplomatik pada dasarnya melindungi kerahasiaan isi komunikasi. Penyesuaian komunikasi digital resmi oleh negara penerima dapat dibaca sebagai pelanggaran langsung terhadap prinsip ini. Dalam kerangka Pasal 27 ayat (2), yang tidak dapat diganggu gugat adalah korespondensi resmi, dan akses tanpa izin terhadap isinya merupakan bentuk gangguan yang paling nyata.

Integritas lebih sulit dijangkau. Konvensi tidak berbicara tentang perubahan isi pesan. Padahal dalam dunia digital, ancaman terbesar kadang bukan pencurian, melainkan pengubahan: dokumen yang dimodifikasi di tengah jalan dapat menyesatkan keputusan negara pengirim. Dapat diargumentasikan bahwa kewajiban "melindungi" komunikasi bebas dalam ayat (1) mencakup perlindungan atas integritasnya, tetapi ini penafsiran yang harus diperkuat, bukan sesuatu yang secara tegas disebut teks.

Ketersediaan menyangkut kemampuan misi untuk tetap dapat berkomunikasi. Serangan yang melumpuhkan jaringan atau layanan, misalnya penolakan layanan terdistribusi (DDoS), tidak membuka isi pesan, tetapi membuat komunikasi bebas tidak mungkin. Ini menyentuh jantung rumusan "mengizinkan dan melindungi komunikasi *bebas*". Di sini kata "bebas" memberi pijakan yang cukup baik: komunikasi yang dilumpuhkan jelas tidak bebas.

Keaslian berkaitan dengan kepastian bahwa pesan memang berasal dari pengirim yang sah. Pemalsuan identitas pengirim, misalnya lewat peretasan akun, tidak tercakup dalam rumusan Pasal 27 secara eksplisit. Ia lebih dekat ke ranah teknis (tanda tangan digital, autentikasi) daripada ranah hukum.

Dari keempat dimensi itu terlihat bahwa Pasal 27 menjangkau kerahasiaan dengan paling meyakinkan, ketersediaan dengan cukup baik, dan baru menyentuh integritas serta keaslian lewat penafsiran. Temuan ini masuk akal: pasal tersebut disusun untuk mencegah *negara*

penerima membuka atau menghalangi komunikasi, bukan untuk menghadapi manipulasi teknis oleh berbagai aktor.

E. Arsip dan Penyimpanan Data: Peran Pasal 24

Bagian yang kerap luput dalam diskusi komunikasi digital adalah arsip. Dahulu, arsip misi tersimpan di ruang aman dalam gedung kedutaan. Kini, sebagian besar arsip berupa berkas elektronik yang disimpan dalam perangkat, server internal, atau layanan cloud milik pihak ketiga.

Pasal 24 menyatakan arsip dan dokumen misi tidak dapat diganggu gugat "kapan pun dan di mana pun berada". Frasa "di mana pun berada" memberi alasan kuat untuk berpendapat bahwa perlindungan arsip tidak berhenti di pagar kedutaan. Arsip yang disimpan di server luar wilayah negara pengirim pun, dari sisi teks, tetap menyandang kedudukan sebagai arsip misi. Pembacaan ini sejalan dengan semangat pasal dan memberi dasar bagi tuntutan bahwa negara penerima, atau negara tempat server berada, tidak boleh menyita atau mengakses data itu.

Walaupun demikian, penerapan praktisnya rumit. Kalau server berada di negara ketiga yang bukan negara penerima, kewajiban siapa yang berlaku? Konvensi mengikat negara penerima terhadap misi yang ditempatkan di wilayahnya, bukan negara ketiga tempat data kebetulan disimpan. Negara ketiga itu mungkin tidak terikat kewajiban khusus terhadap arsip misi, kecuali berdasarkan prinsip umum hukum internasional. Persoalan ini diperburuk bila penyedia cloud adalah perusahaan swasta yang tunduk pada hukum negara asalnya, termasuk kewajiban menyerahkan data atas perintah pengadilan atau lembaga penegak hukum setempat.

Sengketa antara Timor-Leste dan Australia di Mahkamah Internasional (*Questions relating to the Seizure and Detention of Certain Documents and Data*) memberi gambaran yang relevan, meskipun bukan perkara diplomatik dalam arti sempit. Dalam perkara itu, Timor-Leste mempersoalkan penyitaan dokumen dan data elektronik milik penasihat hukumnya oleh aparat Australia pada 2013, dan Mahkamah pada 2014 mengeluarkan penetapan tindakan sementara yang memerintahkan Australia untuk tidak menggunakan materi tersebut dengan merugikan Timor-Leste. Perkara itu kemudian dihentikan setelah para pihak menyelesaikannya pada 2015. Pelajaran pentingnya: Mahkamah menganggap komunikasi rahasia antara suatu negara dan penasihat hukumnya sebagai kepentingan yang layak dilindungi, termasuk ketika berbentuk data elektronik. Perkara ini tidak menyelesaikan persoalan Pasal 27, tetapi menunjukkan bahwa pengadilan internasional siap menilai perlindungan atas data elektronik negara sebagai persoalan hukum yang nyata.

F. Tantangan Hukum Perlindungan Komunikasi Diplomatik Digital

1. Ketiadaan standar teknis dan masalah atribusi

Pasal 27 menetapkan kewajiban, tetapi tidak menetapkan standar. Seberapa kuat enkripsi yang dituntut? Apakah penggunaan aplikasi pesan komersial dapat dianggap sarana yang "layak" untuk informasi rahasia? Konvensi tidak menjawab. Akibatnya, penilaian tentang apakah sebuah negara telah gagal melindungi komunikasi resmi akan selalu memerlukan penafsiran tambahan.

Lebih jauh, hukum internasional tentang tanggung jawab negara menuntut adanya *atribusi*: suatu tindakan baru dapat dibebankan pada negara bila dilakukan oleh organ negara atau pihak yang bertindak atas instruksi, arahan, atau kendali negara. Serangan siber sering dilakukan dengan menyamarkan asalnya, dan membuktikan keterlibatan negara adalah pekerjaan teknis yang sulit. Tallinn Manual 2.0 (Schmitt, 2017) membahas hal ini secara mendalam, termasuk penerapan inviolabilitas misi diplomatik pada operasi siber. Walaupun manual itu bukan dokumen yang mengikat, ia menjadi salah satu rujukan akademik terpenting tentang bagaimana hukum internasional yang ada diterapkan ke ruang siber (Efrony dan Shany, 2018).

2. Pelaku non-negara dan keterlibatan sektor swasta

Pasal 27 terutama ditujukan kepada negara penerima. Namun banyak ancaman digital berasal dari pelaku non-negara: kelompok peretas, penjahat siber, atau kontraktor yang bekerja untuk negara tertentu. Kewajiban negara penerima untuk *melindungi* komunikasi misi sebetulnya dapat dibaca mencakup tindakan pencegahan yang wajar atas gangguan dari pihak-pihak di wilayahnya, tetapi standar kewajaran itu tidak pernah dirumuskan untuk ruang siber.

Di sisi lain, infrastruktur komunikasi hari ini sebagian besar dimiliki dan dioperasikan perusahaan swasta: penyedia internet, platform pesan, dan layanan komputasi awan. Perusahaan-perusahaan itu bukan pihak pada Konvensi Wina dan tidak terikat langsung olehnya. Al-Maadeed (2024) menyoroti persoalan ini sebagai salah satu celah terbesar. Dalam praktik, perlindungan komunikasi diplomatik sangat bergantung pada perjanjian layanan dan kebijakan keamanan perusahaan, yang tidak dibentuk oleh hukum diplomatik.

3. Yurisdiksi data dan lokasi server

Sudah dibahas bahwa Pasal 24 memberi dasar tekstual yang kuat untuk melindungi arsip di mana pun berada. Namun, kekuatan teks tidak otomatis memberi kekuatan penegakan. Bila data misi tersimpan di server di negara ketiga, negara tersebut dapat menerapkan hukumnya sendiri atas data itu, termasuk perintah penyerahan data kepada otoritas. Perdebatan tentang akses lintas batas terhadap data yang disimpan penyedia swasta menunjukkan betapa rumitnya hubungan antara kedaulatan, yurisdiksi, dan lokasi fisik data (Tsagourias dan Buchan, 2021). Persoalan ini tidak dapat dijawab oleh Konvensi Wina yang disusun ketika konsep "lokasi data" belum dikenal.

4. Garis kabur antara komunikasi resmi dan pribadi

Seperti telah disinggung, perlindungan Pasal 27 mengikuti fungsi komunikasi. Diplomat zaman sekarang kerap memakai satu telepon dan satu akun untuk urusan dinas dan pribadi. Bila informasi resmi berada di perangkat yang sama dengan foto keluarga dan percakapan pribadi, pertanyaan tentang apa yang dilindungi dan apa yang tidak menjadi rumit, bukan hanya secara hukum tetapi juga ketika terjadi pemeriksaan perangkat di perbatasan. Kekebalan pribadi diplomat dalam Pasal 29 dan Pasal 30 melindungi diri dan kediaman pribadinya, tetapi bagaimana konsep itu menjangkau isi perangkat bergerak belum diatur jelas. Karena itu, pemisahan perangkat dan akun menjadi langkah praktis yang sangat penting, tidak hanya demi keamanan tetapi juga demi kejelasan status hukum.

5. Perkembangan hukum yang tertinggal dari teknologi

Teknologi berubah dalam hitungan bulan, sedangkan perjanjian multilateral berubah dalam hitungan dekade, itu pun jika ada kemauan politik. Karena itu, mengubah Konvensi Wina 1961 melalui amandemen formal sulit dibayangkan. Konvensi itu sendiri tidak memuat prosedur amandemen khusus, dan membuka kembali teks yang sudah menjadi fondasi hukum diplomatik berisiko menggerus jaminan yang sudah mapan. Banyak negara kemungkinan tidak ingin mempertaruhkan itu.

Atas dasar itu, upaya normatif internasional terkini lebih banyak bergerak di jalur lain. Majelis Umum PBB menerima laporan Kelompok Ahli Pemerintah (GGE) 2021 tentang perilaku negara yang bertanggung jawab di ruang siber, yang menegaskan bahwa hukum internasional, termasuk Piagam PBB, berlaku di ruang siber (United Nations General Assembly, 2021). Laporan akhir Kelompok Kerja Terbuka (OEWG) 2021 menyampaikan pesan senada (United Nations General Assembly, 2021). Pada 2023, Majelis Umum menerima Resolusi 78/16 yang mendorong pembentukan *Programme of Action* sebagai mekanisme dialog tetap tentang perilaku negara dalam penggunaan teknologi informasi dan komunikasi (United Nations General Assembly, 2023). Dokumen-dokumen ini bukan perjanjian mengikat, dan tidak secara khusus membahas Pasal 27. Meskipun begitu, ia menciptakan landasan bersama yang dapat dipakai untuk menafsirkan kewajiban yang sudah ada.

G. Konteks Indonesia

1. Posisi hukum

Sebagai negara pihak pada Konvensi Wina 1961 melalui UU Nomor 1 Tahun 1982, Indonesia memiliki dua peran sekaligus. Sebagai *negara penerima*, Indonesia wajib melindungi komunikasi misi asing di wilayahnya. Sebagai *negara pengirim*, Indonesia berkepentingan agar seluruh perwakilannya di luar negeri dilindungi oleh negara tempat mereka bertugas. Kedua peran ini seharusnya mendorong konsistensi sikap: pandangan yang dikemukakan Indonesia mengenai kewajiban negara penerima akan dibaca orang sebagai ukuran bagaimana Indonesia memperlakukan misi asing.

Pengalaman 2013 memperlihatkan sisi kepentingan Indonesia sebagai negara pengirim. Pemberitaan mengenai dugaan penyadapan terhadap pejabat tinggi

Indonesia oleh badan intelijen Australia memunculkan reaksi diplomatik keras, termasuk pemanggilan duta besar Australia dan penarikan duta besar Indonesia dari Canberra. Pada saat yang sama, peristiwa ini menunjukkan sulitnya penyelesaian hukum. Penyadapan terhadap pejabat tinggi dan penyadapan terhadap misi diplomatik adalah dua hal yang berbeda secara hukum, dan membuktikan pelanggaran dalam kasus semacam itu hampir selalu terbentur masalah bukti yang bersifat rahasia. Sebagian besar penyelesaiannya akhirnya berlangsung melalui jalur politik dan diplomatik, bukan hukum.

2. Kerangka hukum nasional

Mahendra dan Triyana (2025) menemukan bahwa hukum Indonesia belum mengakui kedutaan secara eksplisit sebagai entitas yang dilindungi di ruang siber. Temuan itu masuk akal jika kerangka yang ada diperiksa satu per satu.

Pertama, UU Nomor 37 Tahun 1999 tentang Hubungan Luar Negeri mengatur penyelenggaraan hubungan luar negeri dan kedudukan perwakilan, tetapi disusun pada masa ketika keamanan siber belum menjadi isu kebijakan. *Kedua*, Undang-Undang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dengan UU Nomor 1 Tahun 2024 mengatur transaksi elektronik dan tindak pidana siber secara umum, termasuk akses ilegal dan penyadapan, tetapi tidak membedakan secara khusus komunikasi diplomatik. *Ketiga*, UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi berfokus pada data pribadi warga, bukan data kenegaraan. *Keempat*, Perpres Nomor 82 Tahun 2022 tentang Pelindungan

Infrastruktur Informasi Vital mengatur infrastruktur di sektor-sektor strategis, yang dalam penerapannya berorientasi pada infrastruktur di dalam negeri; belum jelas bagaimana perangkat dan jaringan perwakilan Indonesia di luar negeri diperlakukan. *Kelima*, Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber menyediakan kerangka koordinasi nasional, tetapi dari sisi diplomatik belum merinci mekanisme khusus untuk perwakilan di luar negeri.

Kesimpulannya, Indonesia memiliki sejumlah peraturan yang masing-masing menyentuh sebagian persoalan, tetapi belum ada pengaturan yang secara khusus menggabungkannya untuk melindungi komunikasi diplomatik. Koordinasi antara Badan Siber dan Sandi Negara, Kementerian Luar Negeri, Kepolisian, dan TNI dalam menghadapi serangan terhadap perwakilan diplomatik juga masih terfragmentasi (Mahendra dan Triyana, 2025). Fragmentasi ini berisiko memperlambat respons ketika insiden terjadi, terutama karena serangan siber menuntut keputusan dalam hitungan jam.

3. Peran Indonesia dalam diplomasi digital

Hastri, Hidayat, dan Rofiqi (2024) menekankan bahwa Indonesia sebagai kekuatan menengah perlu memperkuat regulasi dan kebijakan diplomasi digital agar peran strategisnya di forum multilateral tetap terjaga. Argumen ini relevan: negara yang aktif di forum global berkepentingan menunjukkan bahwa komunikasinya dikelola dengan baik. Selain alasan teknis,

ada alasan kredibilitas. Negara yang ingin berpengaruh dalam perumusan norma siber internasional akan lebih meyakinkan jika kebijakan domestiknya sendiri tertata.

H. Upaya Penguatan Perlindungan Komunikasi Diplomatik

Penguatan paling realistis tidak bertumpu pada satu langkah, melainkan pada beberapa lapis yang saling mendukung. Tabel 3 memetakan lapis-lapis itu berdasarkan tingkat dan jangka waktunya.

Tabel 3. Pilihan strategi penguatan perlindungan komunikasi diplomatik digital

Strategi	Tingkat	Jangka waktu	Kelebihan	Keterbatasan
Penafsiran evolutif Pasal 27 (Konvensi Wina 1969, Pasal 31)	Internasional	Segera	Tidak memerlukan perubahan teks; sesuai praktik negara	Tidak menyelesaikan persoalan teknis dan atribusi
Amandemen atau protokol tambahan Konvensi Wina	Internasional	Panjang	Memberi kepastian hukum tertulis	Sulit secara politik; berisiko membuka kembali teks yang sudah mapan
Norma sukarela dan kerja sama (GGE, OEWG, <i>Programme of Action</i>)	Internasional	Menengah	Fleksibel; melibatkan banyak aktor	Tidak mengikat
Protokol keamanan komunikasi resmi di tingkat kementerian	Nasional	Segera	Langsung dapat diterapkan; mengatur perangkat, akun dan penyimpanan	Efektivitas bergantung pada kepatuhan dan pengawasan
Harmonisasi regulasi nasional (UU ITE, UU PDP, Perpres 82/2022, Perpres 47/2023)	Nasional	Menengah	Memberi pijakan hukum domestik yang koheren	Memerlukan koordinasi lintas lembaga
Pelatihan keamanan digital bagi diplomat dan staf	Nasional	Berkelanjutan	Menurunkan risiko kesalahan manusia	Perlu diulang seiring perubahan ancaman
Perjanjian dan pengaturan dengan penyedia layanan swasta	Nasional/bilateral	Menengah	Menjawab celah peran pihak ketiga	Posisi tawar negara terhadap perusahaan besar tidak selalu kuat

Berikut penjelasan lebih rinci atas lapis-lapis tersebut.

Pertama, penafsiran evolutif sebagai fondasi. Seperti dibahas pada bagian B, penafsiran menurut objek dan tujuan serta praktik negara sudah cukup untuk menyatakan bahwa komunikasi elektronik resmi berada dalam perlindungan Pasal 27. Indonesia dapat memperkuat pandangan ini dengan menyatakannya dalam forum seperti Majelis Umum PBB, sehingga praktik dan pernyataan negara-negara terakumulasi menjadi bahan penafsiran yang semakin mantap. Dalam hal ini, Birahayu (2023) benar bahwa revitalisasi hukum tidak selalu harus melalui perubahan teks, tetapi dapat dilakukan melalui praktik negara dan instrumen pelengkap.

Kedua, protokol keamanan resmi. Di tingkat nasional, langkah paling cepat adalah menetapkan aturan yang jelas mengenai perangkat dan akun resmi, pemisahan data dinas dan pribadi, klasifikasi informasi, serta tata cara melapor ketika terjadi insiden. Aturan semacam ini tidak perlu menunggu perubahan undang-undang. Ia dapat dituangkan dalam peraturan menteri atau pedoman internal, dan dapat diperbarui dengan cepat mengikuti perkembangan ancaman.

Ketiga, enkripsi sebagai bagian dari sistem, bukan jawaban tunggal. Enkripsi melindungi isi pesan, tetapi tidak menolong bila perangkatnya sudah diretas atau kata sandinya bocor. Karena itu, enkripsi harus ditempatkan bersama pengamanan perangkat, manajemen akses, dan pembaruan sistem. Pasal 27 ayat (1) yang secara tegas menyebut pesan dalam kode atau sandi dapat dijadikan landasan bahwa penggunaan enkripsi oleh misi diplomatik merupakan hak yang diakui, bukan sesuatu yang perlu dibenarkan kepada negara penerima.

Keempat, sumber daya manusia. Banyak insiden keamanan berawal dari kesalahan sederhana: tautan *phishing* yang dibuka, perangkat yang dipinjamkan, atau kata sandi yang digunakan ulang. Pelatihan berkala bagi diplomat dan staf lokal karena itu sama pentingnya dengan investasi pada perangkat keras. Hukum dapat menjamin kebebasan komunikasi, tetapi kebiasaan penggunaannya yang menentukan apakah jaminan itu bermakna.

Kelima, penanganan insiden dan kerja sama. Perwakilan perlu memiliki prosedur yang jelas ketika terjadi serangan: siapa dihubungi, perangkat mana diisolasi, dan kapan insiden dilaporkan ke pusat. Pada tingkat antarnegara, kerja sama pertukaran informasi ancaman dan pembangunan kapasitas, sebagaimana didorong dalam proses PBB, membantu karena ancaman siber tidak mengenal batas wilayah. Smărăndescu (2025) menekankan bahwa pengembangan norma harus bertahap dan melibatkan negara, organisasi internasional, dan sektor swasta, sebab ancaman terhadap komunikasi diplomatik sering bersifat lintas batas dan melibatkan aktor non-negara.

Keenam, harmonisasi regulasi nasional. Seperti terlihat pada bagian G, peraturan Indonesia yang relevan tersebar. Harmonisasi dapat dilakukan, misalnya, dengan menegaskan bahwa perangkat dan jaringan perwakilan Indonesia di luar negeri diperlakukan sebagai bagian dari infrastruktur informasi yang perlu dilindungi, serta menetapkan mekanisme koordinasi tetap antara Kementerian Luar Negeri dan lembaga keamanan siber. Langkah ini memberi pijakan hukum domestik yang selaras dengan komitmen internasional Indonesia.

Ketujuh, pengaturan dengan penyedia layanan swasta. Karena sebagian besar infrastruktur dimiliki swasta, kontrak dan pengaturan layanan menjadi instrumen perlindungan yang riil. Pemerintah dapat menuntut standar tertentu terkait lokasi penyimpanan, akses oleh pihak ketiga, dan pemberitahuan bila ada permintaan data dari otoritas asing. Jalur ini tidak menggantikan hukum internasional, tetapi mengisi celah yang tidak terjangkau olehnya.

I. Diskusi: Antara Penafsiran dan Pembaruan

Perdebatan tentang perlu tidaknya mengubah Pasal 27 sering terjebak pada pilihan seolah hanya ada dua: tetap atau diubah. Menurut penulis, kerangka itu terlalu sempit. Alasannya ada tiga.

Pertama, nilai terbesar Pasal 27 terletak pada keringkasan dan keumumannya. Rumusan yang tidak menyebut teknologi tertentu justru membuatnya tidak ketinggalan zaman setiap kali ada teknologi baru. Jika teksnya diubah menjadi memuat daftar sarana digital, ia berisiko usang dalam waktu singkat dan perlu direvisi lagi. Pendekatan berbasis prinsip yang dilengkapi pedoman teknis yang mudah diperbarui tampaknya lebih tahan lama.

Kedua, sebagian besar kelemahan yang disorot dalam literatur bukan kelemahan *norma*, tetapi kelemahan *penegakan dan pembuktian*. Masalah atribusi, kerumitan yurisdiksi data, dan peran perusahaan swasta tidak akan hilang walaupun teks Pasal 27 diubah. Menambahkan frasa "komunikasi elektronik" ke dalam pasal tidak akan membuat serangan siber mudah dilacak.

Ketiga, membuka kembali Konvensi Wina 1961 mengandung risiko. Konvensi ini sering disebut sebagai salah satu perjanjian paling berhasil dalam sejarah hukum internasional karena nyaris seluruh negara mematuhi, sebagian karena prinsip timbal balik: setiap negara adalah negara pengirim sekaligus penerima. Proses negosiasi ulang bisa saja dimanfaatkan sebagian negara untuk mempersempit jaminan yang sekarang berlaku. Kehati-hatian karena itu beralasan.

Kendati begitu, penulis tidak berpendapat bahwa tidak ada yang perlu dilakukan. Penafsiran saja menyisakan ketidakpastian, terutama bagi negara yang ingin tahu kapan persisnya suatu tindakan dapat disebut pelanggaran. Itulah mengapa langkah pelengkap, baik berupa kesepakatan politik di forum PBB maupun pedoman praktik negara, tetap diperlukan. Pendapat Mason (2025) dan Al-Maadeed (2024) tentang pembaruan patut dibaca sebagai sinyal kebutuhan akan kepastian, bukan semata-mata tuntutan mengubah teks.

KESIMPULAN

Pertama, Pasal 27 Konvensi Wina 1961 mengatur perlindungan komunikasi diplomatik melalui dua lapis: kewajiban negara penerima untuk mengizinkan dan melindungi komunikasi bebas untuk tujuan resmi, serta larangan mengganggu korespondensi resmi dan kantong diplomatik. Perlindungan ini berlandaskan teori kepentingan fungsional dan diperkuat oleh Pasal 24 mengenai arsip, Pasal 22 mengenai tempat misi, dan Pasal 41 mengenai kewajiban para diplomat.

Kedua, prinsip Pasal 27 tetap relevan bagi komunikasi digital. Frasa *all appropriate means* dan rumusan korespondensi resmi yang berbasis fungsi memungkinkan komunikasi elektronik terlindungi tanpa perubahan teks, sepanjang digunakan untuk keperluan resmi misi. Perlindungan paling kuat berlaku untuk kerahasiaan dan ketersediaan komunikasi, sedangkan integritas dan keaslian baru terjangkau melalui penafsiran. Ketentuan pemancar nirkabel menunjukkan pula bahwa kebebasan komunikasi tidak mutlak.

Ketiga, tantangan hukumnya bukan pada ada tidaknya prinsip, melainkan pada penerapannya: ketiadaan standar teknis, sulitnya atribusi serangan siber, peran pelaku non-negara dan penyedia layanan swasta, rumitnya yurisdiksi atas data, kaburnya batas komunikasi resmi dan pribadi, serta lambatnya perkembangan hukum dibandingkan teknologi. Di Indonesia, tantangan ini diperberat oleh belum adanya pengaturan khusus yang mengakui dan melindungi komunikasi perwakilan diplomatik di ruang siber, serta koordinasi kelembagaan yang masih terpecah.

Keempat, perlindungan yang efektif membutuhkan kombinasi: penafsiran evolutif sebagai fondasi, norma dan kerja sama internasional sebagai pelengkap, protokol keamanan dan pelatihan di tingkat nasional, harmonisasi regulasi domestik, serta pengaturan dengan penyedia layanan swasta.

Saran

1. **Pemerintah Indonesia**, melalui Kementerian Luar Negeri, perlu menyusun pedoman keamanan komunikasi resmi bagi seluruh perwakilan, yang memuat aturan perangkat dan akun resmi, klasifikasi informasi, penyimpanan data, serta prosedur pelaporan insiden.
2. **Pemerintah dan DPR** perlu mengkaji harmonisasi UU Hubungan Luar Negeri, UU ITE, UU PDP, dan peraturan presiden terkait agar perwakilan Indonesia di luar negeri dan komunikasinya memperoleh pijakan hukum yang jelas, serta membentuk mekanisme koordinasi tetap antara Kementerian Luar Negeri, BSSN, dan aparat terkait.
3. **Dalam forum internasional**, Indonesia dapat aktif menyatakan posisi bahwa Pasal 27 dan Pasal 24 Konvensi Wina berlaku bagi komunikasi dan arsip elektronik misi diplomatik, dan mendukung pengembangan norma pelengkap di bawah proses PBB tanpa membuka kembali teks Konvensi.
4. **Peneliti selanjutnya** disarankan melengkapi kajian normatif ini dengan penelitian empiris, misalnya wawancara dengan pejabat Kementerian Luar Negeri dan BSSN, serta kajian perbandingan praktik negara lain dalam mengatur komunikasi digital perwakilannya.

DAFTAR PUSTAKA

Buku

- Bjola, Corneliu, dan Ilan Manor (ed.). *The Oxford Handbook of Digital Diplomacy*. Oxford: Oxford University Press, 2024.a
- Denza, Eileen. *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations*. Edisi ke-4. Oxford: Oxford University Press, 2016.
- Schmitt, Michael N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

Artikel Jurnal

- Al-Maadeed, K. "Diplomatic Law: Between the Constant and the Variable in Light of the New International Order – A Study of Article 27 of the 1961 Vienna Convention on Diplomatic Relations in Light of Technological and Digital Transformations." *Democraticac*, 2024.
- Birahayu, Dita. "Maritime Digital Diplomacy: Legal Revitalization and Reform of Modern and Soluteive Diplomacy." *Audito Comparative Law Journal (ACLJ)* 4, no. 3 (2023): 170-184.
- Hastri, Evi Dwi, Imam Hidayat, dan Imam Rofiqi. "Digital Diplomacy Regulations and Policies: The Middle Power Country's Approach as Indonesia's Multilateral Strategy." *International Journal of Law and Constitution* 1, no. 3 (2024).
- Mason, Robert. "The Vienna Convention Needs an Update to Protect Against AI Threats." *The National Interest*, 27 Agustus 2025.
- Smărandescu, Ioana-Alexandra. "Reinterpreting the Diplomatic Inviolabilities in the Vienna Convention on Diplomatic Relations in the Era of New Technologies." *Romanian Journal of International Law* 33 (2025): 79-96.

Karya Akademik

- Anjani, Daviena Putri, Peni Susetyorini, dan Kholis Roisah. *Dinamika Praktik Diplomasi di Era Digital dalam Perspektif Hukum Diplomatik (Studi Kasus: Persona Non Grata Ebrahim Rasool)*. Skripsi, Fakultas Hukum Universitas Diponegoro, 2026.

Mahendra, Arya Putra, dan Heribertus Jaka Triyana. "Cyber Warfare and Diplomatic Immunity: Evaluating State and Non-State Cyber Operations Targeting Diplomats Under Indonesian Law." ETD Repository Universitas Gadjah Mada, 2025.

Peraturan Perundang-Undangan

Republik Indonesia. Undang-Undang Nomor 1 Tahun 1982 tentang Pengesahan Konvensi Wina mengenai Hubungan Diplomatik Beserta Protokol Opsionalnya Mengenai Hal Memperoleh Kewarganegaraan dan

Pengesahan Konvensi Wina mengenai Hubungan Konsuler Beserta Protokol Opsionalnya Mengenai Hal Memperoleh Kewarganegaraan.

Republik Indonesia. Undang-Undang Nomor 37 Tahun 1999 tentang Hubungan Luar Negeri.

Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024.

Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Republik Indonesia. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital.

Konvensi Internasional

United Nations. Vienna Convention on Diplomatic Relations, 1961.

United Nations. Vienna Convention on the Law of Treaties, 1969.

Dokumen Internasional

International Law Commission. Draft Articles on the Status of the Diplomatic Courier and the Diplomatic Bag Not Accompanied by Diplomatic Courier. Yearbook of the International Law Commission, 1988, vol. II, Part One.

United Nations General Assembly. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. A/76/135, 2021.

United Nations General Assembly. Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security. Resolution 78/16, 2023.

Sumber Institusi

United Nations Institute for Training and Research (UNITAR). Digital and Cyberdiplomacy.

United Nations Office of Information and Communications Technology. ICT Security.

UNESCO. Tech Diplomacy Forum: Building Digital Bridges: Technology, Diplomacy, and Global Cooperation. 2025.